



USPTO

[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

 Search: ☐ The ACM Digital Library ☒ The Guide


THE GUIDE TO COMPUTING LITERATURE


[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

Undetectable on-line password guessing attacks

Full text Pdf (621 KB)

 Source **ACM SIGOPS Operating Systems Review** [archive](#)

 Volume 29 , Issue 4 (October 1995) [table of contents](#)

Pages: 77 - 86

Year of Publication: 1995

ISSN:0163-5980

 Authors **Yun Ding** University of Technology Chemnitz-Zwickau, Chemnitz, Germany

Patrick Horster University of Technology Chemnitz-Zwickau, Chemnitz, Germany

Publisher ACM Press New York, NY, USA

 Additional Information: [abstract](#) [citations](#) [index terms](#) [collaborative colleagues](#) [peer to peer](#)

Tools and Actions:

[Find similar Articles](#) [Review this Article](#)
[Save this Article to a Binder](#) [Display Formats: BibTex](#) [EndNote](#) [ACM Ref](#)

DOI Bookmark:

 Use this link to bookmark this Article: <http://doi.acm.org/10.1145/219282.219298>
[What is a DOI?](#)

↑ ABSTRACT

Several 3-party-based authentication protocols have been proposed, which are resistant to off-line password guessing attacks. We show that they are not resistant to a new type of attack called "undetectable on-line password guessing attack". The authentication server is not able to notice this kind of attack from the clients' (attacker's) requests, because they don't include enough information about the clients (or attacker). Either freshness or authenticity of these requests is not guaranteed. Thus the authentication server responses and leaks verifiable information for an attacker to verify his guess.

↑ CITINGS 4

[Ya-Fen Chang , Chin-Chen Chang, A secure and efficient strong-password authentication protocol, ACM SIGOPS Operating Systems Review, v.38 n.3, p.79-90, July 2004](#)

[Her-Tyan Yeh , Hung-Min Sun, Simple authenticated key agreement protocol resistant to password guessing attacks, ACM SIGOPS Operating Systems Review, v.36 n.4, p.14-22, October 2002](#)

[Chun-Li Lin , Hung-Min Sun , Tzonelih Hwang, Three-party encrypted key exchange: attacks and a solution, ACM SIGOPS Operating Systems Review, v.34 n.4, p.12-20, October 2000](#)

[Ya-Fen Chang , Chin-Chen Chang , Jui-Yi Kuo, A secure one-time password authentication scheme using smart cards without limiting login times, ACM SIGOPS Operating Systems Review, v.38 n.4, p.80-90, October 2004](#)